WHAT IS CLAIMED AND DESIRED TO BE SECURED BY LETTERS PATENT OF THE UNITED STATES IS:

1. An accelerator device, comprising:

an input buffer connected to a packet source and configured to accept and store packets from the packet source;

a scanner configured to scan predetermined fields of the accepted/stored packets; and

a modifier configured to modify fields of packets in said input buffer based on the scanned predetermined fields.

2. The accelerator according to Claim 1, wherein:

said predetermined fields are IPSEC fields of IP packets; and

said modifier comprises a processor configured to at least one of encrypt and decrypt IPSEC fields in said packets.

3. The accelerator according to Claim 2, wherein said modifier is a Mongoose™ type processor.

4. The accelerator according to Claim 1, wherein said scanner scans the predetermined fields of the packets as they are being accepted/stored.

5. The accelerator according to Claim 1, further comprising:

a FIFO configured to store predetermined data from the scanned predetermined fields; and

a state machine configured to retrieve the stored data and program said modifier according to the stored data.

6. The accelerator according to Claim 1, wherein said predetermined data from the scanned predetermined fields comprises a Security Association (SA) ID, a Tx_Pkt_SOP, and flags that indicate if additional fields of the packet need to be scanned to determine information needed for programming said modifier.

7. The accelerator according to Claim 1, further comprising:

a hash state machine configured to generate an SA lookup index (SA ID) based on the predetermined scanned fields.

8. The accelerator according to Claim 1, wherein said hash machine is a polynomial CRC calculation;

9. The accelerator according to Claim 5, wherein:

said predetermined data from the scanned predetermined fields comprises an Rx_Pkt_SOP, and flags that indicate if additional fields of the packet need to be scanned to determine information needed for programming said modifier; and

said modifier is further configured to modify fields of packets in said input buffer based on the SA ID determined by said hash machine.

10. The accelerator according to Claim 1, further comprising:

a FIFO configured to store predetermined data from the scanned predetermined fields; and

a state machine configured to

retrieve data from the FIFO for a particular packet,

read the particular packet from said buffer;

scan additional fields in the particular packet if a flag indicating additional scanning is included in the retrieved FIFO data;

program said modifier to perform one of encryption and decryption of the fields of the packet to be modified according to the retrieved FIFO data and scanned additional fields, and

modify the packet stored in said buffer according to the encrypted or decrypted fields produced by said modifier.

11. A hardware accelerator device, comprising:

parser means connected to an input packet source for parsing predetermined fields of an inbound packet;

hash means for determining a security identification of the inbound packet;

storage means for temporarily storing the parsed predetermined fields and said security identification;

decryption means for deciphering encrypted data of the inbound packet based on programming;

security database means for storing retrievable security associations; and

Control/Data means for,

retrieving security associations from said database,

programming the decryption mechanism based on at least one of the stored security information, other data contained in the incoming packet corresponding to the stored security information, and the retrieved security association, and

modifying fields of the incoming packet based on deciphered output of said decryption mechanism.

12. A method of performing IPSEC processing, comprising:

scanning a packet for IPSEC related information

programming an IPSEC services device to perform IPSEC processing based on the scanned IPSEC information; and

providing data from said packet for processing by the IPSEC services device; and

modifying said packet based on an output from the IPSEC security services device;

wherein said steps of scanning, programming, providing, and modifying are performed by a hardware device at an IP layer of a network connected device.

13. The method according to Claim 12, wherein said IPSEC security services device is a Mongoose™ device.

14. The method according to Claim 12, wherein said IPSEC related information comprises data contained in at least one of Authentication (AH), and Encapsulating Security Payload (ESP) fields of said packet.

15. The method according to Claim 12, wherein said step of programming includes the steps of,

determining a security association by indexing a security association database with at least part of the scanned IPSEC related information, and

providing the determined security association to the IPSEC services device.

16. The method according to Claim 12, further comprising the steps of:

hashing at least one field of said packet to determine a security association ID (SA ID);

determining a security association by looking up a security association in an SA database based on the SA ID; and

utilizing the security association as part of the programming provided to the security services device.

17. The method according to Claim 1, wherein:

said step of scanning comprises scanning said packet as it is being received from a packet source; and

said packet source is one of a network card and upper layers of a host protocol stack.

18. The method according to Claim 1, wherein said step of providing comprises the steps of:

reading at least part of said packet from a buffer device storing said packet; and

providing at least part of the data read as input to said IPSEC security services device.

19. The method according to Claim 1, wherein said steps of scanning, programming, providing, and modifying are performed within the IP layer of the network protocol stack.

20. The method according to Claim 1, wherein said step of modifying comprises:

when said packet is using Encapsulating Security Payload and said packet is in transport mode,

adding ESP, ESP Trailer, and ESP Auth fields to said packet,

encrypting the ESP, TCP, Data, and ESP Trailer fields, and

authenticating the ESP, TCP, Data, and ESP Trailer fields;

when said packet is using Encapsulating Security Payload and when said packet is in tunnel mode,

adding a new IP header, ESP, ESP Trailer, and ESP Auth fields to said packet,

encrypting the original IP header, TCP, Data, and ESP Trailer fields of said packet, and

authenticating the ESP, original IP header, TCP, Data, and ESP Trailer fields of said packet;

when said packet is using Authentication Header and said packet is in transport mode,

adding an AH field, and authenticating the entire packet except for mutable fields; and

when said packet is using Authentication Header and said packet is in tunnel mode,

adding a new IP Header and AH field, and authenticating the entire packet except for mutable fields.

21. The method according to Claim 1, wherein said step of modifying comprises writing at least portions of said packet that are being added and/or modified by the security services device to a buffer storing said packet prior to shipment of said packet to one of a transport device or upper layer protocols of a host device.